

Exhibit 2

US Patent No. 7,137,140 v. Adyen

Claim	Analysis
<p>[25.1] A method of operating a network system comprising a first computer arrangement and a second computer arrangement connected by a computer network, wherein:</p>	<p>Adyen performs and induces other to perform a method of operating a network system comprising a first computer arrangement and a second computer arrangement connected by a computer network.</p> <p>For example, Adyen provides a Risk Management solution which includes Device Fingerprinting (includes java script files) for merchants and PSPs (Payment Service Providers) to identify and reduce risks to online businesses. Adyen utilizes signals from a user's computing device such as PC, laptop and/or mobile devices ("first computer arrangement") to prevent fraud on online commerce and/or PSPs. The user's computing device is connected to the merchant and/or PSPs' server and Adyen's server ("second computer arrangement") by a computer network.</p>

The screenshot shows a web browser displaying the Adyen Risk management documentation at <https://docs.adyen.com/risk-management>. The page has a dark header with the Adyen logo and a search bar. The main content area features a large heading "Risk management" with a lightning bolt icon, followed by a brief description and a paragraph about maintaining fraud defenses. Below this, there are three sections: "Dynamic 3D Secure and AVS", "Disputes", and "ShopperDNA". Each section contains a brief description and a link to more information.

Source: <https://docs.adyen.com/risk-management>

	<h2>Risk checks</h2> <p>The risk engine has numerous rules available for configuration that are assessed at the time of a transaction. These risk checks are outlined in a list of RevenueProtect engine rules. Many risk checks require you to provide additional information on the payment to perform better assessment of the transaction. For more information, see Provide data for risk checks. You can also skip risk checks.</p> <p>Risk checks can be performed in batches across lists of referrals using the Referral list API. It is also possible to manually review a transaction before it is captured. This is an optional, yet powerful second layer of enforcement that can go on top of standard risk checks. For more information, see Case Management - Manual Review.</p> <p>If you want to use our risk system for payments processed by another PSP, our standalone risk solution allows you to make risk only calls to the Adyen payments platform.</p> <hr/> <h2>Risk profiles</h2> <p>Create and use risk profiles to work in tandem with risk checks. Risk profiles allow you to manage risk settings across multiple merchant accounts, or to apply a different set of risk settings for a specific payment.</p> <p>Source: https://docs.adyen.com/risk-management</p>
[25.2] the first computer arrangement requests data be transferred from the second computer arrangement to the first computer arrangement;	<p>Adyen performs and induces others to perform the step of the first computer arrangement requests data be transferred from the second computer arrangement to the first computer arrangement.</p> <p>For example, when a user tries to buy goods or services (“data”) from a merchant and/or PSPs website integrated with Adyen’s Risk Management solution (includes Device Fingerprinting), on a computer, laptop or any other computing device, the computing device requests for the data to be transferred from merchant and/or PSPs’ server to the user’s computing device.</p>

Home / Risk management / Device fingerprinting



Device fingerprinting

Device Fingerprinting allows you to log unique attributes of the shopper device and analyze them during repeat visits of the same shopper. This helps the [ShopperDNA system](#) identify the same machine across multiple sessions (despite the user changing login identities, using proxies, clearing cache and cookies, and attempting other obfuscation techniques) and detect fraudulent behavior easily on a payment page.

Adyen provides you with the following options depending on the integration type you use:

- For [HTML-based Client-Side Encryption](#) and [Hosted Payment Pages](#), the device fingerprint is calculated and submitted automatically.
- For [JavaScript-only Client-Side Encryption](#) and [Direct API](#), you need to manually calculate and submit the fingerprint, as shown in this document.

Get the fingerprint

First, calculate a fingerprint on a client side and submit it to your server, along with other payment details. Note that calculating the device fingerprint might take some time varying on the shopper's computer speed and Internet connection. We recommend that you call the fingerprinting code on the page load to make sure that the fingerprint has been successfully calculated while a shopper fills out payment details.

Source: <https://docs.adyen.com/risk-management/device-fingerprinting>

Get the fingerprint

First, calculate a fingerprint on a client side and submit it to your server, along with other payment details. Note that calculating the device fingerprint might take some time varying on the shopper's computer speed and Internet connection. We recommend that you call the fingerprinting code on the page load to make sure that the fingerprint has been successfully calculated while a shopper fills out payment details.

To get the device fingerprint:

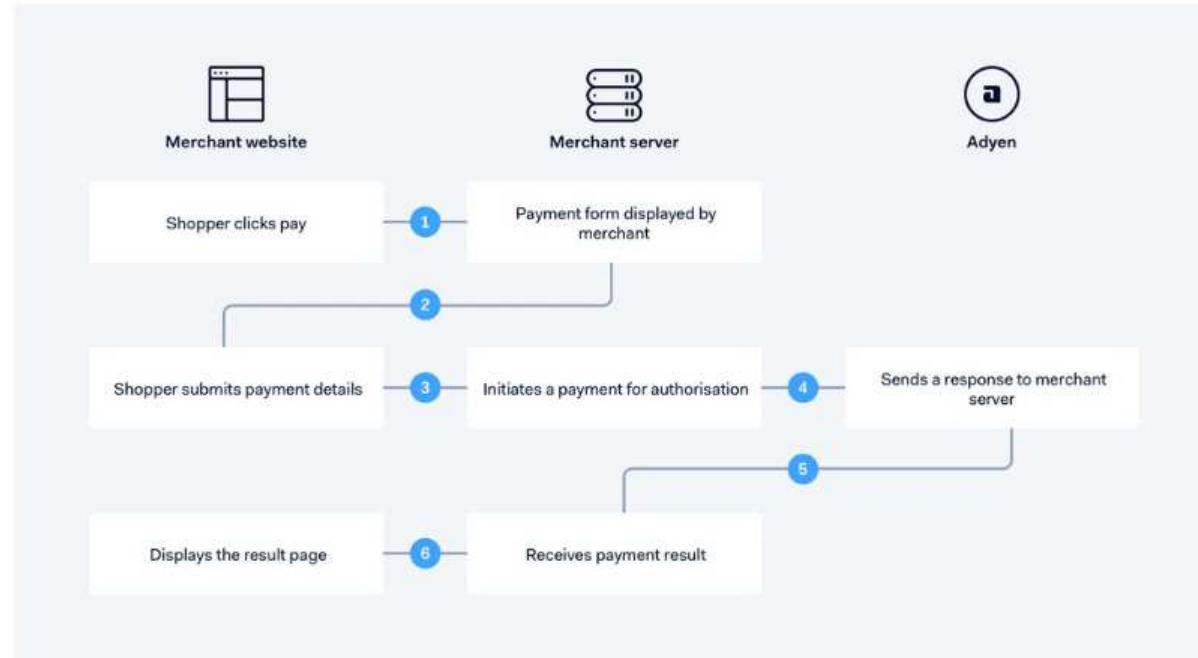
1. Add a reference to the <https://live.adyen.com/hpp/js/df.js> script to your Checkout page. Browsers typically cache JavaScript files, so we recommend specifying the current date (YYYYMMDD) in the URL (for instance, <https://live.adyen.com/hpp/js/df.js?v=20171130>). This ensures you benefit from future updates to the calculation of the device fingerprint.
2. Add a hidden field with any `id` to your page.
3. Calculate a fingerprint for the hidden field by calling the `dfDo` function with the field's `id` as a parameter.



The JavaScript file that calculates the device fingerprint has been minified to reduce loading time.

Source: <https://docs.adyen.com/risk-management/device-fingerprinting>

Your card payments go through many stages. The diagram below helps you understand the flow:



Source: <https://docs.adyen.com/classic-integration/api-integration-ecommerce>

[25.3] in response to the request, the second computer arrangement transmits executable fingerprint software from the second computer arrangement to the first computer arrangement;	<p>Adyen performs and induces others to perform the step in response to the request, the second computer arrangement transmits executable fingerprint software from the second computer arrangement to the first computer arrangement.</p> <p>For example, in response to the request, the merchant and/or PSPs' server transmits a java script file ("executable fingerprint software") such as df.js, which is added to the Checkout page of the merchant website on the user's computing device.</p>
--	---

Home / Risk management / Device fingerprinting



Device fingerprinting

Device Fingerprinting allows you to log unique attributes of the shopper device and analyze them during repeat visits of the same shopper. This helps the [ShopperDNA system](#) identify the same machine across multiple sessions (despite the user changing login identities, using proxies, clearing cache and cookies, and attempting other obfuscation techniques) and detect fraudulent behavior easily on a payment page.

Adyen provides you with the following options depending on the integration type you use:

- For [HTML-based Client-Side Encryption](#) and [Hosted Payment Pages](#), the device fingerprint is calculated and submitted automatically.
- For [JavaScript-only Client-Side Encryption](#) and [Direct API](#), you need to manually calculate and submit the fingerprint, as shown in this document.

Get the fingerprint

First, calculate a fingerprint on a client side and submit it to your server, along with other payment details. Note that calculating the device fingerprint might take some time varying on the shopper's computer speed and Internet connection. We recommend that you call the fingerprinting code on the page load to make sure that the fingerprint has been successfully calculated while a shopper fills out payment details.

Source: <https://docs.adyen.com/risk-management/device-fingerprinting>

Get the fingerprint

First, calculate a fingerprint on a client side and submit it to your server, along with other payment details. Note that calculating the device fingerprint might take some time varying on the shopper's computer speed and Internet connection. We recommend that you call the fingerprinting code on the page load to make sure that the fingerprint has been successfully calculated while a shopper fills out payment details.

To get the device fingerprint:

1. Add a reference to the <https://live.adyen.com/hpp/js/df.js> script to your Checkout page. Browsers typically cache JavaScript files, so we recommend specifying the current date (YYYYMMDD) in the URL (for instance, <https://live.adyen.com/hpp/js/df.js?v=20171130>). This ensures you benefit from future updates to the calculation of the device fingerprint.
2. Add a hidden field with any `id` to your page.
3. Calculate a fingerprint for the hidden field by calling the `dfDo` function with the field's `id` as a parameter.



The JavaScript file that calculates the device fingerprint has been minified to reduce loading time.

Source: <https://docs.adyen.com/risk-management/device-fingerprinting>

Home / Risk management / Device fingerprinting

Below is an example form that calculates the device fingerprint using the `bar` hidden field.

```
1  <html>
2  <head>
3      <title>Your Website</title>
4  </head>
5  <body><p>Your Checkout page.</p>
6      <script type="text/javascript" src="https://live.adyen.com/hpp/js/df.js?v=20171130"></script>
7      <form action="http://www.yourdomain.com/checkout" method="POST">
8          <!--
9              Your other payment related fields
10             -->
11         <input type="hidden" name="foo" id="bar" />
12         <input type="submit" value="Submit" />
13     </form>
14     <script>
15         //<![CDATA[
16         dfDo("bar");
17         //]]&gt;
18     &lt;/script&gt;
19     &lt;/body&gt;
20 &lt;/html&gt;</pre>
```

Source: <https://docs.adyen.com/risk-management/device-fingerprinting>

<p>[25.4] the first computer arrangement executes the executable fingerprint software by reading and performing the plurality of instructions and thereby creates fingerprint data that is substantially unique to the first computer arrangement and transmits the fingerprint data to the second computer arrangement,</p>	<p>Adyen performs and induces others to perform the step of the first computer arrangement executes the executable fingerprint software by reading and performing the plurality of instructions and thereby creates fingerprint data that is substantially unique to the first computer arrangement and transmits the fingerprint data to the second computer arrangement.</p> <p>For example, the user's computing device executes the java script (such as df.js) to generate a substantially unique fingerprint data (such as device parameters and/or browser features) for each device during checkout. The device fingerprint is calculated by adding a reference to the df.js script to the checkout page. The hidden field is added with any id to the merchant's browser page and fingerprint is calculated for the hidden field by calling the dfDo function with the field's id as a parameter. The fingerprint data is sent to the Adyen's server.</p> <h3>Get the fingerprint</h3> <p>First, calculate a fingerprint on a client side and submit it to your server, along with other payment details. Note that calculating the device fingerprint might take some time varying on the shopper's computer speed and Internet connection. We recommend that you call the fingerprinting code on the page load to make sure that the fingerprint has been successfully calculated while a shopper fills out payment details.</p> <p>To get the device fingerprint:</p> <ol style="list-style-type: none"> 1. Add a reference to the https://live.adyen.com/hpp/js/df.js script to your Checkout page. Browsers typically cache JavaScript files, so we recommend specifying the current date (YYYYMMDD) in the URL (for instance, https://live.adyen.com/hpp/js/df.js?v=20171130). This ensures you benefit from future updates to the calculation of the device fingerprint. 2. Add a hidden field with any <code>id</code> to your page. 3. Calculate a fingerprint for the hidden field by calling the <code>dfDo</code> function with the field's <code>id</code> as a parameter. <p> The JavaScript file that calculates the device fingerprint has been minified to reduce loading time.</p> <p>Source: https://docs.adyen.com/risk-management/device-fingerprinting</p>
--	---

Home / Risk management / Device fingerprinting

Below is an example form that calculates the device fingerprint using the `bar` hidden field.

```
1 <html>
2   <head>
3     <title>Your Website</title>
4   </head>
5   <body><!--><p>Your Checkout page.</p>
6   <script type="text/javascript" src="https://live.adyen.com/hpp/js/df.js?v=20171130"></sc
7   <form action="http://www.yourdomain.com/checkout" method="POST">
8     <!--
9       Your other payment related fields
10      -->
11     <input type="hidden" name="foo" id="bar" />
12     <input type="submit" value="Submit" />
13   </form>
14   <script>
15     //<![CDATA[
16     dfDo("bar");
17     //]]&gt;
18   &lt;/script&gt;
19 &lt;/body&gt;
20 &lt;/html&gt;</pre>
```

Source: <https://docs.adyen.com/risk-management/device-fingerprinting>

Home / Risk management / Device fingerprinting

Submit the fingerprint to Adyen

After the device fingerprint is calculated and submitted to your server, include this fingerprint into the payment request in the `deviceFingerprint` field value. The Adyen payments platform then uses this fingerprint for fraud checks on the payment request.

JSON **SOAP**

```
1  {
2      "amount":{
3          "currency":"EUR",
4          "value":"2000"
5      },
6      "card":{
7          "cvc":"737",
8          "expiryMonth":"08",
9          "expiryYear":"2018",
10         "holderName":"Adyen Test",
11         "number":"4111111111111111"
12     },
13     "merchantAccount":"YourMerchant",
14     "reference":"Your Reference Here",
15     "shopperEmail":"s.hopper@test.com",
16     "shopperIP":"61.294.12.12",
17     "shopperReference":"Simon Hopper",
18     "deviceFingerprint":"m7Cmrff++0cW4P6XFF7m/rA"
19 }
```

Source: <https://docs.adyen.com/risk-management/device-fingerprinting>

	<p>Your card payments go through many stages. The diagram below helps you understand the flow:</p> <pre> graph TD subgraph Merchant [Merchant] direction TB MWebsite["Merchant website"] --- MPForm["Payment form displayed by merchant"] MPForm --- MServer["Merchant server"] MServer --- MAdyen["Adyen"] end subgraph Adyen direction TB AdyenIcon["Adyen"] end MWebsite -- "1. Shopper clicks pay" --> MPForm MPForm -- "2. Shopper submits payment details" --> MServer MServer -- "3. Initiates a payment for authorisation" --> AdyenIcon AdyenIcon -- "4. Sends a response to merchant server" --> MServer MServer -- "5. Receives payment result" --> MResult["Displays the result page"] MResult -- "6. Displays the result page" --> MPForm </pre> <p>Source: https://docs.adyen.com/classic-integration/api-integration-ecommerce</p>
[25.5] the second computer arrangement receives the fingerprint data from the first computer arrangement; and	<p>Adyen performs and induces others to perform the step of the second computer arrangement receives the fingerprint data from the first computer arrangement.</p> <p>For example, the fingerprint data is received at the Adyen's server from the user's computing device using merchant's website.</p>

Home / Risk management / Device fingerprinting

Submit the fingerprint to Adyen

After the device fingerprint is calculated and submitted to your server, include this fingerprint into the payment request in the `deviceFingerprint` field value. The Adyen payments platform then uses this fingerprint for fraud checks on the payment request.

JSON **SOAP**

```
1  {
2      "amount":{
3          "currency":"EUR",
4          "value":"2000"
5      },
6      "card":{
7          "cvc":"737",
8          "expiryMonth":"08",
9          "expiryYear":"2018",
10         "holderName":"Adyen Test",
11         "number":"4111111111111111"
12     },
13     "merchantAccount":"YourMerchant",
14     "reference":"Your Reference Here",
15     "shopperEmail":"s.hopper@test.com",
16     "shopperIP":"61.294.12.12",
17     "shopperReference":"Simon Hopper",
18     "deviceFingerprint":"m7Cmrff++0cW4P6XFF7m/rA"
19 }
```

Source: <https://docs.adyen.com/risk-management/device-fingerprinting>

	<p>Your card payments go through many stages. The diagram below helps you understand the flow:</p> <pre> graph TD subgraph "Merchant website" direction TB A[Shopper clicks pay] -- 1 --> B["Payment form displayed by merchant"] end subgraph "Merchant server" direction TB C[Shopper submits payment details] -- 2 --> D[Initiates a payment for authorisation] D -- 3 --> E["Sends a response to merchant server"] end subgraph "Adyen" F[Receives payment result] G[Displays the result page] E -- 4 --> F F -- 5 --> G end </pre> <p>Source: https://docs.adyen.com/classic-integration/api-integration-ecommerce</p>
[25.6] in response to receiving the fingerprint data, the second computer arrangement transmits the requested data	<p>Adyen performs and induces others to perform the step in response to receiving the fingerprint data, the second computer arrangement transmits the requested data from the second computer arrangement to the first computer arrangement.</p> <p>For example, in response to receiving the fingerprint data at Adyen's server, Adyen then returns a result page through the merchant and/or PSPs' server. Once the customer/user's device is allowed by matching device</p>

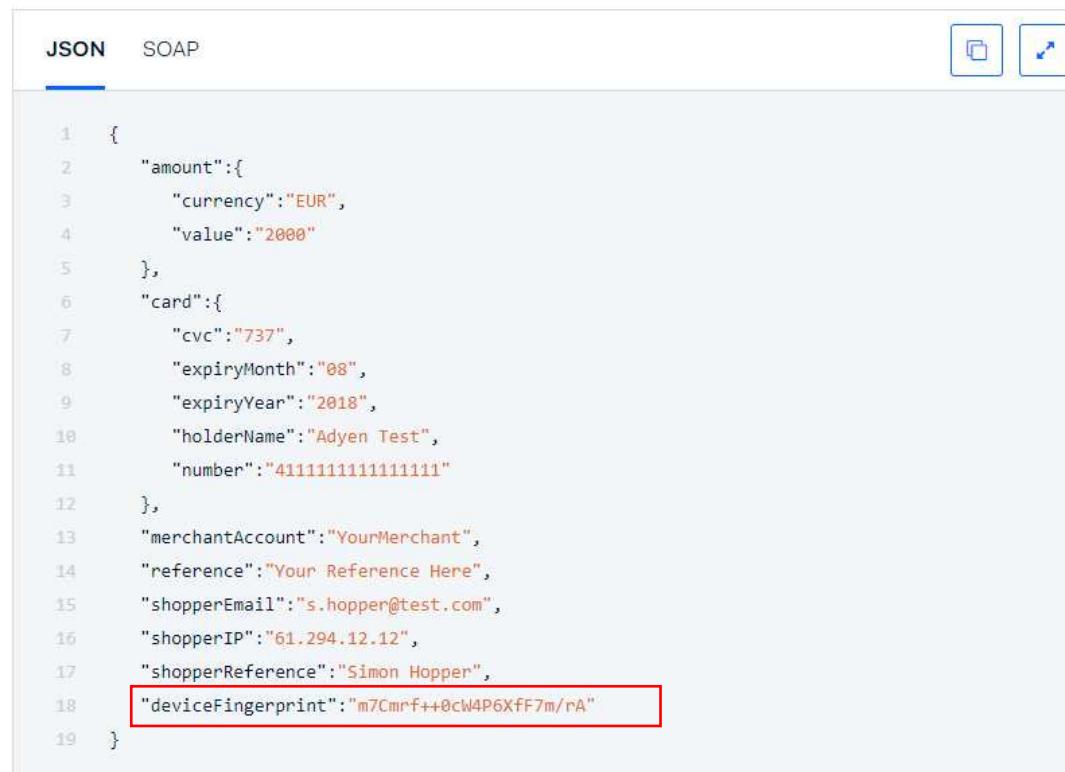
from the second computer arrangement to the first computer arrangement.

fingerprint with the stored fingerprint at Adyen's server, the requested data is sent from the merchant and/or PSPs' server to the user's computing device.

[Home](#) / [Risk management](#) / [Device fingerprinting](#)

Submit the fingerprint to Adyen

After the device fingerprint is calculated and submitted to your server, include this fingerprint into the payment request in the `deviceFingerprint` field value. The Adyen payments platform then uses this fingerprint for fraud checks on the payment request.



```

JSON      SOAP
1  {
2    "amount":{
3      "currency":"EUR",
4      "value":"2000"
5    },
6    "card":{
7      "cvc":"737",
8      "expiryMonth":"08",
9      "expiryYear":"2018",
10     "holderName":"Adyen Test",
11     "number":"4111111111111111"
12   },
13   "merchantAccount":"YourMerchant",
14   "reference":"Your Reference Here",
15   "shopperEmail":"s.hopper@test.com",
16   "shopperIP":"61.294.12.12",
17   "shopperReference":"Simon Hopper",
18   "deviceFingerprint":"m7Cmrff++0cW4P6Xff7m/rA"
19 }

```

Source: <https://docs.adyen.com/risk-management/device-fingerprinting>

